



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,718	03/18/2004	Kevin Eugene Dombkowski	LUC-469/Dombkowski 11-16	6988
32205 7590 12/18/2007 PATTI, HEWITT & AREZINA LLC ONE NORTH LASALLE STREET 44TH FLOOR CHICAGO, IL 60602			EXAMINER YALEW, FIKREMARIAM A	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 12/18/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/803,718

Applicant(s)

DOMBKOWSKI ET AL.

Examiner

Fikremariam Yalew

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. The office action is in reply to an amendment filed on 10/10/2007. Claims 1-5,7-12,14-15,21-22 have been amended. Claim 23 is new added. Claims 1-23 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 22 are directed to a computer-readable medium. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. Claim 22 is directed a computer readable medium that includes data signals (See page 18 line 22 through page 19 line). A signal does not fall within one of the statutory classes of 101. Claim 22 is rejected as being directed to a computer-readable medium that include data signals.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-6,8-18,20-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Karaoguz(US Pub No 2004/0059914 A1) in view of Mackenzie et al(hereinafter referred as Mackenzie et al(hereinafter referred as Mackenzie) US Pub No 2002/0141594 A1.

7. As per claims 1,14,22: Karaoguz discloses an apparatus/method/article, comprising: an authentication device that authenticates a computing device (See 0041 0049), in communication with the authentication device, through employment of a determination that a current location of the authentication device matches an initial location of the authentication device (See Fig 3 steps 305,310,335 and Fig 4 steps 440 and 0019).

Karagouz does not explicitly teach wherein one or more private keys employable for encryption and /or decryption of information are erased upon an attempt to move the authentication device. However Mackenzie teaches wherein one or more private keys employable for encryption and /or decryption of information are erased upon an attempt to move the authentication device (See col 4 lines 44-47 and col 12 lines 6-16).

Therefore it would have been obvious to one ordinary skill in art at that time the invention was made to modify the teaching method of Mackenzie within Karaoguz method inorder to provide enhancing security for the system.

8. As per claim 2: the combination of Karaoguz and Mackenzie disclose the apparatus wherein the computing device comprises a first computing device wherein the authentication device makes the determination that the current location of the authentication device matches the initial location of the authentication device in response to a request from a second computing device for authentication of the first computing device for a data transfer from the second computing device to the first computing device (See Karaoguz 0008,0019-0020).

9. As per claims 3,15: the combination of Karaoguz and Mackenzie disclose the apparatus/method wherein the request from the second computing device comprises an authentication challenge string (See 0038,0041); wherein the authentication device stores one or more private keys, wherein if the current location of the authentication device matches the initial location of the authentication device, then the authentication device employs one or more of the one or more private keys to decrypt the authentication challenge string into an authentication challenge response(See Karaoguz 0038).

10. As per claims 4,16: the combination of Karaoguz and Mackenzie disclose the apparatus/method wherein the authentication device sends the authentication challenge response to the second computing device, wherein the second computing device analyzes the authentication challenge response to determine whether the first computing device is authenticated for the data transfer (See Karaoguz 0037-0038).

11. As per claims 5,17: the combination of Karaoguz and Mackenzie disclose the apparatus/method wherein the second computing device comprises an authentication challenge key to compare with the authentication challenge response received from the authentication device (See Karaoguz 0038,0041); wherein if the authentication challenge

response matches the authentication challenge key, then the authentication challenge response represents that the first computing device is authenticated and the data transfer can be sent from the second computing device to the first computing device(See Karaoguz Fig 4 step 440 and 0038,0041).

12. As per claims 6,18: the combination of Karaoguz and Mackenzie disclose the apparatus wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device prevents authentication of the first computing device and disables the one or more private keys (See Karaoguz Fig 4 step 450 and 0042).

13. As per claim 8,20: the combination of Karaoguz and Mackenzie disclose the apparatus/method wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the computing device; wherein the base portion is fixed to a surface near the computing device, wherein the cover portion is fixed to the base portion to provide a secure shell for the one or more electronic components (See Karaoguz Figs 2,3 and 0017,0050).

14. As per claim 9,21: the combination of Karaoguz and Mackenzie disclose the apparatus/method wherein a first one of the base and cover portions receives electricity through a power port, wherein a second one of the base and cover portions receives electricity through an electrical contact with the first one of the base and cover portions(See Karaoguz Fig 5 step 515,525); wherein upon separation of the second one of the base and cover portions from the first one of the base and cover portions, the second one of the base and cover portions loses power and prevents authentication of the computing device(See Karaoguz Fig 5 step 515,525).

15. As per claim 10: the combination of Karaoguz and Mackenzie disclose wherein the second one of the base and cover portions electrically supports one or more of the one or more electronic components that store one or more private keys, wherein the authentication device employs one or more of the one or more private keys to authenticate the computing device (See Karaoguz Fig 5 step 515,525); wherein a loss of power in the second one of the base and cover portions erases the one or more private keys from the one or more of the one or more electronic components(See Karaoguz Fig 5 step 515,525).

16. As per claim 11: the combination of Karaoguz and Mackenzie disclose the apparatus wherein the authentication device comprises a location sensor (See Karaoguz 0039); wherein upon initialization of the authentication device, the location sensor sets the initial location of the authentication device (See Karaoguz 0039,0045); wherein the location sensor determines the current location of the authentication device, wherein the authentication device compares the current location with the initial location to authenticate the computing device (See Karaoguz 0039,0045).

12. As per claim 12: the combination of Karaoguz and Mackenzie disclose the apparatus wherein the location sensor comprises a global positioning system component, wherein the global positioning system component measures the initial location and the current location of the authentication device as a three-dimensional location of latitude, longitude, and altitude (See Karaoguz 0045-0046).

13. As per claim 13: the combination of Karaoguz and Mackenzie disclose the apparatus wherein the authentication device allows authentication of the computing

device upon the determination that the authentication device matches the initial location of the authentication device within a specified error message (See Karaoguz 0039,0045)

17. As per claim 23: the combination of Karaoguz and Mackenzie disclose the apparatus wherein the one or more private keys are erased upon an attempt of open the authentication device (See Mackenzie US Pub No 2002/0141594 A).

18. Claims 7,19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Karaoguz(US Pub No 2004/0059914 A1) in view of Mackenzie et al(hereinafter referred as Mackenzie et al(hereinafter referred as Mackenzie) US Pub No 2002/0141594 A1 and further in view of Wheeler et al(US Pub No 2007/0088950 A1.

19. As per claims 7,19: the combination of Karaoguz and Mackenzie disclose claims 6 and 15 as recited above. The combination of Karaoguz and Mackenzie do not explicitly teach the apparatus wherein the authentication device stores the one or more private keys in volatile memory, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys.

However Wheeler the apparatus wherein the authentication device stores the one or more private keys in volatile memory, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys(See 0146).

Therefore it would have been obvious to one ordinary skill in art at that time the invention was made to modify the teaching method of Wheeler within Karaoguz and Mackezie method in order to provide enhancing security for the system.

Conclusion

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

Fikremariam Yalew
02/14/2007
FA

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Art Unit 2136


12,17,07